

## ABSTRACT

Methods and apparatuses are disclosed for improving DES and other cryptographic protocols against external monitoring attacks by reducing the amount (and  
5 signal-to-noise ratio) of useful information leaked during processing. An improved DES implementation of the invention instead uses two 56-bit keys (K1 and K2) and two 64-bit plaintext messages (M1 and M2), each associated with a permutation (i.e., K1P, K2P and M1P, M2P) such that  $K1P\{K1\} \text{ XOR } K2P\{K2\}$  equals the "standard" DES key K, and  $M1P\{M1\} \text{ XOR } M2P\{M2\}$  equals the "standard" message. During operation of the  
10 device, the tables are preferably periodically updated, by introducing fresh entropy into the tables faster than information leaks out, so that attackers will not be able to obtain the table contents by analysis of measurements. The technique is implementable in cryptographic smartcards, tamper resistant chips, and secure processing systems of all kinds.